An introduction to information security

An introduction to information security

Open University

978 1 47300 164 0 (epub)
978 1 47300 069 8 (kdl)

1.0

Contents

Introduction

Information security underpins the commercial viability and profitability of enterprises of all sizes and the effectiveness of public sector organisations. This unit begins by explaining why information security and its management are important for any modern organisation. The unit continues by examining the value that can be placed on information as an organisational asset. The protection of information assets is the subject of the BSi standard on information security management, and the unit goes on to explain how an information security management system should be planned, documented, implemented and improved, according to the standard. This unit is based on readings from the book *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799* (2nd edition) by Alan Calder and Steve Watkins (Kogan Page, 2003). In order to study this unit you will need to buy this set book. You will also need to pay if you want access to the British Standard (mentioned above) using British Standards Online.

This unit is an adapted extract from the course Information security management (M886)

Learning outcomes

By the end of this unit you should have developed an understanding of

- how you select appropriate techniques to tackle and solve problems in the discipline of information security management;
- why security and its management are important for any modern organisation;
- how an information security management system should be planned, documented, implemented and improved, according to the BSi standard on information security management.

1 Why is information security important?

This unit introduces you to information security and its management

A succinct definition of *information security* might run as follows

> Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure

But why is it important to secure information? And how should its security be managed? To start thinking about these questions, consider the following statements about *information*

> In today's high technology environment, organisations are becoming more and more dependent on their information systems The public is increasingly concerned about the proper use of information, particularly personal data The threats to information systems from criminals and terrorists are increasing Many organisations will identify information as an area of their operation that needs to be protected as part of their system of internal control
>
> (Nigel Turnbull, 2003, p xi)

> Competitive advantage … is dependent on superior access to information
>
> (Robert M Grant, 2000, p 186)

> Information is the oxygen of the modern age It seeps through the walls topped by barbed wire, it wafts across the

electrified borders

(Ronald Reagan, 1989)

It is vital to be worried about information security because much of the value of a business is concentrated in the value of its information. Information is, as Grant says, the basis of competitive advantage. And in the not-for-profit sector, with increased public awareness of identity theft and the power of information, it is also, as Turnbull claims, the area of an organisation's operations that most needs control. Without information, neither businesses nor the not-for-profit sector could function. Valuing and protecting information are crucial tasks for the modern organisation.

If information were easy to value and protect, however, you would be able to buy off-the-shelf information security management solutions. There are three characteristics of information security that make this impossible.

1. The collection of influences to which each organisation is exposed varies with the organisation: the information technology that it uses, its personnel, the area in which it does business, its physical location – all these have an effect on information security.
2. Information security affects every structural and behavioural aspect of an organisation: a gap in a security fence can permit information to be stolen, a virally infected computer connected to an organisation's network can destroy information, a cup of coffee spilt on a computer keyboard can prevent access to information.
3. Each individual that interacts with an organisation in any way – from the potential customer browsing the website, to the managing director, from the malicious hacker, to the information

security manager – will make his or her own positive or negative contribution to the information security of the organisation

Thus information security and its management need to be examined within an organisational context To this end, a major aim of this unit is to give you the opportunity to:

- investigate your organisation and determine the precise mix of information security issues that affect it;
- explain the links between areas of an organisation and navigate your organisation's information security web;
- identify the security contributions of each individual, and so suggest strategies to make the sum of the positive contributions greater than the sum of the negative ones.

Before you can investigate information security and its management within your organisation, we need to introduce you in more detail to the complexities of the topic This is the purpose of this unit. Section 2 discusses the meaning of the terms information, information security and information security management Section 3 looks at information security and its imperatives and incentives Section 4 discusses information assets Section 5 examines the planning of an information security management system Section 6 addresses how risks to information security can be assessed and how information assets can be identified Section 7 describes how a system for information security management can be implemented and continually improved

2 Information, information security and information security management

2.1 What is information?

Information comprises the meanings and interpretations that people place upon facts, or data The value of information springs from the ways it is interpreted and applied to make products, to provide services, and so on

Many modern writers look at organisations in terms of the use they make of information For instance, one particularly successful model of business is based on the assets that a firm owns Assets have traditionally meant tangible things like money, property, plant, systems, but business analysts have increasingly recognised that information is itself an asset, crucial to adding value As Grant said in Section 1, information underpins competitive advantage Indeed, there are writers, such as Itami and Roehl (1987), who believe that the true value of an organisation is in the information it uses and creates

But, of course, there is a negative side too the use of information in both the for-profit and not-for-profit sectors is increasingly the subject of legislation and regulation, in recognition of the damage its misuse can have on individuals

Note: All activities in this unit consist of a statement of the activity followed by some guidance and/or a discussion You should read the guidance *before* attempting the activity, and the discussion *after* attempting it

Activity 1

(a) In your Learning Journal, write down the main objective – sometimes called the mission – of your organisation.

(b) List the main kinds of information your organisation requires to meet its mission. Note down any areas in which the mission makes preserving the value of information difficult.

(c) Read the Introduction to *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 177799* (2nd edition) by Alan Calder and Steve Watkins (the Set Book) and make notes on why information is important to a modern organisation.

Guidance

1. Your answer to (b) will depend on the nature of your organisation. If your organisation produces a product, you may be able to identify information that is used in the creation of the product, including intellectual property such as designs and patents. If your organisation is a retailer, appropriate information might include customer information and price lists. A not-for-profit organisation will perhaps have employee lists, client lists, stock lists, a charter, etc. All for-profit organisations are required to keep financial information.
2. Don't worry if you feel that you take little from your reading of the Introduction to the Set Book at this stage. We suggest that you make a note to reread the material, and to refer back to the notes that you made, once you have completed this unit. You are likely to find that you are then better able to appreciate the arguments presented.

View discussion

2.2 What is information security?

Seen in the way we have just defined it, information is a valuable asset. *Information security* protects information (and the facilities and systems that store, use and transmit it) from a wide range of threats, in order to preserve its value to an organisation.

This definition of information security is adapted from that of the American National Security Telecommunications and Information Systems Security Committee (NSTISSC).

There are two important characteristics of information that determine its value to an organisation:

- the *scarcity* of the information outside the organisation;
- the *shareability* of the information within the organisation, or some part of it.

Simplifying somewhat, these characteristics state that information is only valuable if it provides advantage or utility to those who have it, compared with those who don't.

Thus the value of any piece of information relates to its levels of shareability and scarcity. The aim of information security is to preserve the value of information by ensuring that these levels are correctly identified and preserved.

Threats to information influence the organisation's ability to share it within, or to preserve its scarcity outside. And threats that are carried out can cost millions in compensation and reputation, and may even jeopardise an institution's ability to survive. Here are some examples in which the making available of information that should have been kept scarce or the restricting of information that should have been shareable has damaged an organisation.

Example 1: Softbank – theft of consumer data for extortion

Softbank of Japan offers broadband internet services across Japan through two subsidiaries – Yahoo! BB and Softbank BB. In February 2004, the bank announced that the security of 4.5 million customer records had been compromised: data from both subsidiaries had been illegally copied and disseminated. The leaked details included customer names, home phone numbers, addresses and email IDs, but did not include passwords, access logs or credit card details.

Softbank became aware of the problem only when they were approached by two groups of extortionists. The criminals produced apparently genuine customer data and threatened that all of the data would be posted to the internet if they were not paid a large sum of money.

Japanese police made three arrests but suspected that there may have been connections to organised crime and the political far-right. Amazingly, the police concluded that there had in fact been two simultaneous, yet independent, extortion attempts against Softbank, both of them masterminded by employees of the company. All of the people accused of extortion had been authorised to access the customer data, but it appeared that Softbank had inadequate procedures to protect against its unwarranted copying and dissemination.

The bank immediately announced a tightening of security, further restricting access to their systems and enforcing tighter security on all of their subsidiaries Profuse apologies were offered to the affected customers and ¥4 billion (£20 million) were paid in compensation Furthermore, Softbank BB's president, Masayoshi Son, announced that he and other senior executives would take a 50 per cent pay cut for the next six months

In this example, the threat was to reduce the value of an organisation by revealing information that should have been a well-kept secret – scarce-within as well as scarce-without It cost the company £20 million in compensation and affected its reputation

Example 2: UCSF Medical Center

In October 2002, the University of California, San Francisco (UCSF) Medical Center received an email message from someone who claimed to be a doctor working in Pakistan and who threatened to release patient records onto the internet unless money owing to her was paid Several confidential medical transcripts were attached to the email

UCSF staff were mystified, they had no dealings in Pakistan and certainly did not employ the person who sent the email The Medical Center began an immediate investigation, concentrating on their transcription service, which had been outsourced to Transcription Stat, based in nearby Sausalito It transpired that Transcription Stat farmed out work to some fifteen subcontractors scattered across America One of these subcontractors was Florida-based Sonya Newburn, who in turn employed further subcontractors, including one Tom Spires of Texas No one at Transcription Stat realised that Spires also employed his own subcontractors, including the sender of the email. The sender alleged that Spires owed her money, and had not paid her for some time

Newburn eventually agreed to pay the $500 that the email sender claimed was owed to her. In return the sender informed UCSF that she had had no intention of publicising personal information and had destroyed any records in her care. Of course, there is no way to prove that the records have actually been destroyed.

Naturally, you would not wish your own medical records to be publicised: they should be scarce. This threat cost the organisation little in money terms, but how much in reputation? Just what is a reputation worth? Or, to put it another way, how much is it worth paying in information security to protect a reputation?

Example 3: Logic bombs

In May 2000, Timothy Lloyd was found guilty of causing between $10 million and $12 million worth of damage to Omega Engineering, an American company specialising in precision engineering for clients, including the US Navy and NASA. Lloyd had been employed with Omega for 11 years, rising to the post of system administrator, and was responsible not only for the day-to-day operation of the company's computers but also for their disaster-recovery process.

In 1996, Lloyd became aware that he was about to be sacked and wrote a logic bomb – a six-line destructive program – which he installed on Omega's servers. Ten days later, Lloyd was dismissed and his logic bomb exploded, destroying company contracts and proprietary software used by Omega's manufacturing tools. Although Omega had instituted a backup procedure, Lloyd's account privileges had allowed him to disable these recovery systems. The damage done by his logic bomb was permanent.

When the logic bomb 'exploded' it wiped out information that was needed for the company to operate. As a result of lost business, Omega was forced to lay off some 80 employees and found itself rewriting the very software which had once given it a competitive edge over its rivals. In effect, what Lloyd managed to do, in the most decisive way possible, was to prevent vital information being shared.

Activity 2

Read the Foreword to *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799* (the Set Book), written by Nigel Turnbull.

> (a) Write down the three reasons Turnbull gives for companies recognising the need to protect information.
>
> (b) Write down two of the ways in which this unit should be valuable to you and your own organisation.

Guidance

You may wish to discuss your answer to (b) with other learners, using the Comments section below.

View discussion

2.3 What is information security management?

Information security management is the process by which the value of each of an organisation's information assets is assessed and, if appropriate, protected on an ongoing basis. The information an organisation holds will be stored, used and transmitted using various media, some of which will be tangible – paper, for example – and some intangible – such as the ideas in employees' minds. Preserving the value of information is mainly a question of protecting the media in which it is contained.

Building an information security management system (as we present it in this unit) is achieved through the systematic assessment of the systems, technologies and media used for information assets, the appraisal of the costs of security breaches, and the development and deployment of countermeasures to threats. Put simply, information security management recognises the most vulnerable spots in an organisation and builds armour-plating to protect them.

The diversity of the media used for an organisation's information assets is just one of the difficulties to be overcome in building an information security management system. Among other difficulties are the following.

- Effective information security measures often run counter to the mission of an organisation. For instance, the safest way to secure a computer and the information on it is to allow no access to it at all!
- The requirement to respect the needs of the users of the organisation's information, so that they can continue to do their jobs properly.

We can deduce that no single solution can address all possible security concerns The only strategy is to engineer a fit-for-purpose solution that achieves a suitable balance between risks and protection against them

As with all management systems, the engineering of a fit-for-purpose information security management system is achieved through hard work Part of the hard work is, of course, an understanding of the technologies involved – we provide the necessary details in this unit. Other major tasks are identifying the needs of the different stakeholders and ensuring coverage of every procedure and policy that involves the development, transformation or dissemination of sensitive information

Thus, information security management is a development activity analogous to the development of software, and we shall present in this way throughout this unit.

Activity 3

Click on **Reading 1** to read the section from the introduction to the British Standard on Information Security Management entitled 'What is information security?'.

Click below to open Reading 1 (0 2 MB)

Reading 1

1. How is information security characterised in the Standard?
2. How is information security achieved, according to the Standard?

Guidance

1. The original standard on information security management

that was developed by the British Standards Institute (BSI) was British Standard BS 7799–1:1999. This was revised as International Standard ISO/IEC 17799:2000(E), and then readopted in the UK as British Standard BS 7799–1:2000 (and is also referred to as BS ISO/IEC 17799:2000). Subsequently a second standard, BS 7799–2:2002, was developed (based on an earlier standard, BS 7799–2:1999, brought out to accompany BS 7799–1:1999), creating the current two-part British Standard on information security management. We shall refer to these two documents collectively as the British Standard on Information Security Management, or as the Standard for short. Individually, we shall refer to BS 7799–1:2000 as Part 1 of the Standard and BS 7799–2:2002 as Part 2 of the Standard. Both parts of the Standard are accessible from British Standards Online. It is a section from the Introduction to Part 1 of the Standard (BS 7799–1:2000) that you are asked to read here.

2. When reading the extract, try not to be put off by its dry and formal style and language.

View discussion

3 Information security imperatives and incentives

3.1 Introduction

The design of a successful information security policy and strategy for any organisation requires an assessment of a number of key factors. These factors can be categorised as either *imperatives* or *incentives*. Imperatives are pressures that force you to act. Incentives are the rewards and opportunities that arise from acting.

In Subsection 3.2 we examine the main imperatives confronting organisations. These arise either from threats to information assets or from the obligation to comply with UK law and with codes governing the management and control of public and private assets and the protection of the interests of stakeholders. We place all of these imperatives in a wider framework of ethical practice in information management.

In Subsection 3.3 we look briefly at some of the incentives for engaging in information security management. Incentives mainly come in the form of opportunities to reduce the cost of existing ways of working and new options for pursuing an organisation's objectives.

3.2 Imperatives

Imperatives generally arise from three sources:

1. **threats:** companies that depend on information and the technologies that carry it have to protect these resources from a wide range of threats;
2. **legislation:** many countries have enacted legislation to govern the storage and use of information;
3. **regulation:** many countries have regulations governing the management and control of public and private assets.

Chapters 1 and 2 of *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799* highlight some of the main imperatives facing organisations in the UK. Chapter 1 presents a case for action based upon likely threats and the need to comply with current legislation. Citing industry surveys, it gives an account of the prevalence of threats, introducing two specific categories: *cybercrime* and *cyberwar*. Chapter 2 expands the authors' case, describing the obligation of many UK organisations to comply with the Combined Code, the recommendations of the Turnbull Report and the public-sector equivalents of these. You will be asked to read these chapters as you study this section.

3.2.1 Threats

Activity 4

Read Chapter 1 of the Set Book and evaluate the case for information security made in that chapter.

Guidance

To complete this activity, you should consider carefully the statistics the authors present. Do try to be critical. Try to distinguish the points that you feel are made convincingly from those that might warrant deeper enquiry or scrutiny. Ask yourself about the motives and interests of the parties whose research and opinions are presented. Do you think the evidence is presented in a balanced way?

There is no need to be exhaustive. Aim for about three or four substantial observations that you could discuss with a colleague, or with other learners. You may wish to use the Comments section below to air your views.

View discussion

3.2.2. Legislation

In Chapter 1 of *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799* (the Set Book), the section entitled 'Legislation' lists the UK legislation that affects the management of information security. One way to appreciate the relevance of legislation to an organisation is to identify the rights and entitlements it establishes and then to establish whether the organisation or its stakeholders have an interest in those rights and entitlements. For each law considered, Table 1 identifies, in general terms, the legal rights established and the parties whose interests are protected by it.

Table

Law	Rights established
Data Protection Act 1998	Protects individuals against the use of personal information by another individual or organisation.
Freedom of Information Act 2000	Provides individuals with the right of access to information held by public authorities and those providing services for them.
Computer Misuse Act 1990	Protects the right of individuals and organisations to preserve the confidentiality and integrity of their computer data.
Copyright Designs and	Protects intellectual property, i.e. protects the interests of an individual, or an organisation that employs such individuals, whose

Patents Act 1988	ownership of novel, creative or inventive work is recognised in law
Electronic Communications Act 2000	Protects the interests of society by restricting the use of cryptographic techniques so that the Government and its authorised agents are able to decrypt any message that is legitimately intercepted.
Human Rights Act 1998	Protects the right of individuals against unreasonable disruption of and intrusion into their lives, while balancing this individual right with those of others
Regulation of Investigatory Powers Act 2000	Protects the originators of electronic communication from its interception without lawful authority and protects employees from unreasonable monitoring
Public Interest Disclosure Act 1998	Protects employees who, in the public interest, disclose criminal or civil wrongdoing by their employer.

We include this final law for completeness. It is not listed in the section on 'Legislation' in Chapter 1, but is mentioned in the 'Intellectual property rights (IPR)' section of Chapter 27.

Activity 5

Read the sections entitled 'Identification of applicable legislation' and 'Intellectual property rights (IPR)' at the start of Chapter 27 of the Set Book. Then, in light of your reading and for each law identified in Table 1, try to give one example of how it affects your organisation's use of information.

Guidance

You might find it helpful to discuss this activity with other learners, using the Comments section below.

View discussion

3.2.3. Regulation and codes of conduct

Chapter 1 of the Set Book presents a case for effective information security based largely upon perceived threats and legal obligations. Chapter 2 introduces further imperatives, which govern specific types of organisation in the UK

Activity 6

Read Chapter 2 of the Set Book

(a) Identify the imperatives that are relevant to each of the following types of organisation:

- publicly listed company (plc)
- organisation in supply-chain relation with a plc
- UK Government (HMG)
- non-governmental organisation (NGO)
- non-departmental public body (NDPB)
- organisation in supply-chain relation with HMG, NGO, NDPB

Note: The supply chain for an organisation is the set of other organisations involved in the creation, by the original organisation, of a product or service.

(b) Describe how the Turnbull Report affects your organisation.

Guidance

1. The 'Orange Book' referred to in the Set Book is more properly known as *Management of Risk – A Strategic Overview* published by HM Treasury in 2001. (Note: In the context of computer security, the term 'Orange Book' originally referred to the U.S. National Computer Security Center's 1985 publication *U.S. Department of Defense, Trusted Computer System Evaluation Criteria*, but has since been appropriated as a shorthand for similar documents.)
2. Recall that an *imperative* is a pressure that forces you to act. Thus, for example, an imperative for the UK Government in this context is that it must comply with the Turnbull Report, adapted in the form of the Orange Book.
3. Chapter 2 of the Set Book describes the impact of the Turnbull Report on for-profit organisations in some detail, while simply mentioning that it applies to not-for-profit organisations. If you work in the not-for-profit sector, you may wish to consult colleagues within your organisation to help you to answer (b).

View discussion

3.2.4. Ethics

The Turnbull Report, and a series of other codes relating to corporate governance, highlight some of the ethical principles which guide managers in the public and private sectors. In many cases, such codes are produced only after crises have occurred. Much legislation comes about in the same way. Information security management also has an ethical aspect, not least because of the need to apply the ethical spirit of laws and codes of conduct in new and unfamiliar circumstances.

The Organisation for Economic Co-operation and Development (OECD) produced in 2002 the document *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Principle 4 of which has this to say on ethics:

> **Participants should respect the legitimate interests of others.**
>
> Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

The OECD document can be found at

http://www.oecd.org/document/42/0,3343,en_2649_201185_15582250_1_1_1_1,00.html (accessed 3 April 2008).

Activity 7

Write down what you think 'ethical conduct' means in practice.

Guidance

If you are a member of a professional body, you may be able to refer to its definition of ethical conduct. If not, you may like to look in a dictionary or other reference book for a definition of 'ethics' or 'ethical', and try to apply it to your role within your organisation. You may also be able to use 'ethical conduct' as a search term on the Web.

View discussion

3.3 Incentives

Activity 8

Reread the short section entitled 'Benefits of an information security management system' at the end of Chapter 1 of *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book). In light of your reading, write down, in your own words, the benefits of an information security management system for your organisation.

View discussion

4 Information assets

4.1 Introduction

Section 2 explained that information is an important asset to an organisation. In this section you will study, in some detail, the characteristics of information assets that make them valuable, and so worth protecting.

In recent years, a combination of computerised processing systems and electronic communication technologies has made possible new forms of working and trading based on the electronic exchange of information. Such activity is called *e-business* or *e-commerce*. Two new, but already familiar, models of organisations working together electronically in this way are the following.

- **Business-to-business (b2b) commerce,** in which businesses work closely together, using the internet, to trade information, services and/or products. Examples include financial management and Web-server management.
- **Business-to-customer (b2c) commerce,** in which the internet is used to connect a business directly to the customer without the need for premises such as shops or warehouses. Examples include many small software firms, the book retailer Amazon and economy airlines.

Despite their names, these models apply to not-for-profit as well as for-profit organisations. For example, the Open University makes use of the b2c model.

The OASIS Universal Description, Discovery and Integration (UDDI) protocol is a directory service that enables organisations and applications to find and use Web services over the internet. The supporting website (http //uddi xml org) has an interesting collection of white papers on the technologies involved and their use

Of course the electronic exchange of information takes place within individual organisations as well as between them, typically reducing communication delays For example separate business units within a company use email to transfer documents almost instantly, whereas in the past they had to rely on a comparatively slow internal mail system Highly efficient intraorganisational workflows are now possible through electronic communication

However, these new forms of communication and commerce also present new dangers since they make an organisation's information assets subject to new threats Access to vital assets may no longer be restricted to those who have a key for the lock of the door that protects a building Electronic communication may make the whole world your market place, but there is a danger that it will also make the whole world your premises

In this section we shall examine the characteristics of information assets that make them worth protecting We shall also discuss the concepts of shareability, scarcity, confidentiality, integrity and availability in relation to these assets

4.2 Information in an e-business age

Sharing information in business is itself a risky business The information that is exchanged between b2b partners, for instance, may include order information, customer details and strategic documents Such information could be priceless to outsiders As you saw in the previous section, huge costs can result from information getting into the wrong hands

In sharing information, an organisation also needs to be aware of the various laws, regulatory frameworks and codes of practice Failure to comply with these can lead to disciplinary action against individuals and to legal action against organisations In such situations, directors and managers are duty bound to be cautious and vigilant.

But the rewards of the e-business age can be immense Information has become a powerful source of competitive advantage, and may contribute massively to the value of an organisation and to its ability to meet its mission And this is not just theory. One only needs to look at the difference between the *book value* of an organisation – the value placed on it by accountants – and its *market value* – the value placed on it by investors – to see the significance of information For instance, in 1997 Coca-Cola had a market value of $33 4 billion, whereas its book value was only just above $1 2 billion intangible assets, including information, contributed to over $30 billion of additional value In the same year, Microsoft had a market valuation 21 4 times its book value Intangible assets, such as information, expertise and the company's huge customer base, made up the difference.

So, clearly, information assets are important But what counts as an information asset? Part 1 of the British Standard on Information Security Management offers numerous examples

These assets are listed as item (a) in **Reading 2** (linked below), the section 'Inventory of Assets' from Part 1 of the Standard; a similar list appears on page 96 of *IT Governance A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book)

Click below to open Reading 2 (0 3 MB).

Reading 2

Activity 9

(a) Which information assets, do you think, contribute most to (i) Coca-Cola's and (ii) Microsoft's value?

(b) List the information assets that you think contribute most to your organisation's value

Guidance

For (a), you may wish to use the internet to help you develop your answer

For (b), you may need to consult colleagues at work to help you with your assessment

View discussion

With tangible assets – everything from office supplies to heavy machinery – the fact that they occupy physical space means that their theft has an obvious effect: quite simply, the asset disappears. Interference with information assets, on the other hand, is not so easily detected. A piece of information does not disappear if it is copied, even if that copying is a form of theft, neither does a computer file change or disappear if it is duplicated. Many of the forms in which information is stored, such as word-processing files, show no traces when they have been interfered with or changed. Even an unauthorised person looking over your shoulder as you read an electronic or paper document may be stealing information without you noticing that they are doing so. Moreover, it is quite possible that the systems that receive, host, manipulate and transmit your organisation's information assets could be tampered with without showing any discernible difference in their structure or behaviour, so that all your valuable information assets could be copied to someone inside or outside of your organisation without your being aware of it until it is too late. One example of this sort of tampering is *spyware*, which is unauthorised software installed on your computer with the aim of allowing someone at a distance to see what you are doing on your computer. For instance, spyware can record the keystrokes you make as you edit a document, allowing them to be played back on another system to recreate that document.

Activity 10

(a) What precautions do you, or could you, take to assure yourself that there is no spyware on your computer at the moment?

(b) Find out about your organisation's current position on spyware and protection against it.

View discussion

4.3 Scarcity and shareability

Modern business theory now views an organisation's intangible, rather than its tangible, assets as the reservoir of much of its value. Even a not-for-profit organisation requires information to be shared and protected for its mission to be accomplished. With this new perspective has come a re-evaluation of the methods to be used to protect the value of an organisation. Historically, four walls were all that was needed to demarcate the inside of an organisation from the outside, and four sturdy walls were all the protection necessary for complete safety. Today, it is those with whom the organisation shares information, and those from whom it keeps it secret, that determine organisational boundaries.

The existence of such organisational boundaries led Grant (1996) to the following observations concerning assets (in the most general sense):

- assets should be *shareable* (i.e. available for use) within the organisation, or some part of it;
- assets should be *scarce* (i.e. not available for use) outside the organisation.

You met these concepts in Subsection 2.2.

Grant goes on to assert that, in for-profit organisations, the combination of shareability and scarcity is the basis of competitive advantage. In not-for-profit organisations, shareability of information contributes to the discharge of the organisation's mission, and its scarcity is often required by law or by other codes.

We can elaborate Grant's argument. Any information asset has two regions associated with it. First, it has a *shareability region* that contains all the systems and people to which and to whom the information asset should be available. Second, it has a *scarcity region*, containing *all other* systems and people.

To maximise an information asset's utility (and thus its value) to an organisation, it should be available within its shareability region whenever needed. If such an asset is not available when some authorised person or system requests it, then this is a failure of shareability. You will have experienced such failures yourselves: not having access to your email when you need it, for example, or not being able to remember your password for some machine or system. In a wider context, an inaccessible customer or product database may have a serious impact on an organisation's ability to carry out its mission.

Moreover, for it to be useful to an organisation, an information asset should always be *correct* within its shareability region If it becomes corrupted or damaged in some way it will be less useful, or even worthless For example, you undoubtedly have had personal experience of word-processed documents that are unopenable, or can be accessed but have been corrupted in some way

An information asset should either be unavailable in its scarcity region or, if needs dictate that it must be available it should be damaged or disabled in some way to remove its value as far as the organisation that owns it is concerned Examples of information that has to be released into its scarcity region are easy to find in the commercial world especially on the internet *Demoware*, for instance, is commercial software that has had some important function disabled, so that it can be freely distributed for demonstration purposes while ensuring that anyone who finds it useful has to pay a licence fee for the complete version

Activity 11

(a) Identify one information asset that is valuable to your organisation Explain why you feel it to be valuable

(b) Is the information asset you have chosen shareable? Is it scarce? Draw a diagram showing the shareability and scarcity regions in which you would place yourself, your organisation, your contacts, and other elements of your organisation's environment, with respect to this asset

(c) Consider the diagram you have drawn Do the shareability and scarcity regions overlap? Does the shareability region correspond to any recognisable unit of activity in your organisation?

(d) How much control does an organisation have over the shareability and scarcity regions of its information assets?

Guidance

1. To identify a valuable information asset for your organisation, you could start from your organisation's mission and consider which information assets contribute most to it.
2. To determine the asset's shareability and scarcity, consider whether it is commercially sensitive and/or covered by legislation, codes of practice, etc.

View discussion

4.3.1 Confidentiality, integrity and availability

To preserve the value of an information asset, an organisation needs to sustain simultaneously its scarcity and its shareability within their respective regions. This is the critical high-level information security goal for any information asset; it is the entire rationale of an information security management system.

To maintain the security of an information asset, an organisation must:

- *either* make the information asset unavailable in its scarcity region, i.e. make it *confidential* to the shareability region,
- *or* damage or disable the information asset before allowing it into the scarcity region, i.e. undermine the *integrity* of the asset. The damage or disablement must be such that the original information asset retains most, or all, of its value to the organisation.

At the same time, to ensure that an information asset maintains its value, an organisation must:

- ensure that the information asset is *available* within the shareability region;
- maintain the *integrity* of the information asset within the shareability region.

Most authors accept that confidentiality, integrity and availability are the most important information security requirements – requirements rather than goals, because they can, in principle, be controlled directly by an organisation. Because of this, they form the basis of most modern approaches to information security management, including that of the British Standard on Information Security Management, which provides good definitions of all three terms. The definitions appear in Reading 1, 'What is information security?', at the start of the Introduction to Part 1 of the Standard.

Information security management is therefore concerned with ensuring an information asset's confidentiality, availability and integrity, and breaches in information security can be defined as a reduction in one or more of these three features. Thus, breaches of an information asset's security requirements have occurred when:

- the confidentiality of the information asset is reduced by it being disclosed outside its shareability region;
- the integrity of the information asset is harmed by it being corrupted or damaged inside its shareability region;
- the integrity of the information asset is preserved after it has crossed from the shareability to the scarcity region;
- the availability of the information asset is reduced inside its shareability region.

In addition, the availability of an information asset can be reduced by

- the destruction or loss of the information asset, the hardware it resides upon, or the software that interacts with it;
- the interruption, for a period of time, of access to the information asset.

The security requirements of an information asset may change over time, as may its value to an organisation. Consider this simple example relating to the confidentiality of an information asset. Suppose you have information that a company is soon due to make an announcement that will cause its stock price to rise or fall. The fact that one could make a killing on the stock market with such information makes it very valuable, and so subject to the highest levels of confidentiality. However, after the official announcement, the information loses its value, and so the requirement of confidentiality is no longer an issue. *Insider dealing*, which includes the inappropriate release of such information, is a criminal offence under the Criminal Justice Act 1993. Similarly, time can affect the security requirements regarding availability and integrity: the need for an information asset to be available will be greater at some times than others, as will the need for its integrity.

Activity 12

(a) Explain how the goals of shareability and scarcity for an information asset can be achieved in terms of the security requirements of confidentiality, integrity and availability.

(b) Do you think these three security requirements apply to non-information assets?

(c) Choose an example of an information asset valuable to your organisation. To which of the three security requirements is it subject?

(d) Assess how the security requirements for the information asset you chose change overtime.

(e) What are the possible results of a breach of the security requirements of an information asset?

View discussion

5 Planning an information security management system

5.1 Introduction

In this section you will study the process demanded by the British Standard on Information Security Management for planning an information security management system (ISMS). We present ISMS development as a process involving four tasks, each of which may be subdivided into stages. This section also examines the managerial and organisational structures that the Standard recommends to support ISMS development and looks in detail at the ISMS documentation task.

5.2 The Standard's approach to planning an ISMS

The Standard describes the planning of an ISMS, which it refers to as the 'Plan activity', as follows:

> The Plan activity ... is designed to ensure that the context and scope for the ISMS have been correctly established, that all information security risks are identified and assessed, and that a plan for the appropriate treatment of these risks is developed. It is important that all stages of the Plan activity are documented for traceability and for the management of change.
>
> (Part 2 of the Standard, Annex B.2.1, p. 22)

This description suggests an approach to the planning and documentation of an ISMS that comprises four tasks. These four tasks are not identified explicitly in the Standard. The *documentation* task, which takes place throughout the process, can be summarised as follows.

- *ISMS documentation*, in which the context and scope of the ISMS, and its rules for assessing risk, are determined and in which the documentation that makes progress through the stages of the process traceable and the management of change possible is generated.

This task begins at the same time as, runs in parallel with, and records the decisions of the three other tasks, which take place sequentially and concern the *planning* of the ISMS.

- *Asset identification*, in which the information assets that are to be handled by the ISMS are identified, and their security requirements are established.
- *Risk assessment*, in which the risks of breaches of the security requirements of information assets are assessed.
- *Risk treatment*, in which a plan for the management of the risks is developed.

The planning tasks complement and drive the documentation task, by providing the operational details of what the ISMS will do.

The relationships between the four tasks are illustrated in Figure 2.

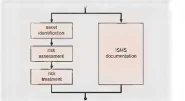


Figure 2 The relationships between the four tasks comprising the ISMS planning and documentation process

The four tasks are subdivided into stages, each of which is described in Clause 4.2.1 of Part 2 of the Standard.

5.2.1 ISMS documentation

ISMS documentation is carried out at organisation level. Its purpose is to define the scope and context of the proposed system, and the approach to information security management that it will embody. It has five stages: three that initiate the planning process (Stages 1 to 3) and two that complete it (Stages 8 and 9).

> **Stage 1: define the scope of the ISMS** The context and scope of the ISMS are defined by considering the nature of the organisation, the business (or service) area in which it operates, and its location, assets and technology. The scope of the ISMS is a statement of which information assets are to be protected (Clause 4.2.1(a))

Stage 2: define an ISMS policy An ISMS policy, often referred to simply as an information security policy, is drawn up. This important document underpins the ISMS and contributes to the traceability and repeatability of its processes. It should, among other things, set up criteria against which security risks to information assets can be evaluated. (Clause 4.2.1(b))

Stage 3: define a systematic approach to risk assessment A document specifying a systematic approach to risk assessment is written. This must include a process for evaluating the likelihood of a risk to an information asset's security requirements, and the impact of a breach of them, along with a definition of what constitutes acceptable risk. (Clause 4.2.1(c))

Stage 8: prepare a Statement of Applicability The Statement of Applicability of the ISMS is completed, based on information gathered at Stage 7 (during risk treatment). (An explanation of what is meant by a Statement of Applicability is given in Subsection 5.4.) (Clause 4.2.1(h))

Stage 9: obtain management approval The complete ISMS documentation, consisting of the papers drawn up in Stages 1, 2, 3 and 8, is submitted to senior management for approval. (Clause 4.2.1(i))

5.2.2 Asset identification

The asset identification task is carried out at unit level within an organisation, in light of organisation-wide policies set out in Stages 1 to 3. It uses Stage 1's description of the scope of the ISMS to determine the information assets that are to be protected.

Stage 4.1: identify the assets at risk The information assets at risk are identified, along with their owners, their locations, their values and their information security requirements. The results are documented (Clause 4 2 1(d)(1))

5.2.3 Risk assessment

The risk assessment task is also carried out at unit level, in light of policies set out in Stages 1 to 3 and for the assets identified in Stage 4.1

Stages 4.2, 4.3 and 4.4: identify the risks

Stage 4.2 determines systematically the possible threats to the assets identified in the asset identification part of the process (Clause 4 2 1(d)(2))

Stage 4.3 identifies vulnerabilities that might allow those threats to become successful attacks on the assets. (Clause 4 2 1(d)(3))

Stage 4.4 uses the evaluation mechanisms established in Stage 3 to assess the impact of breaches of the assets' security requirements (Clause 4 2 1(d)(4))

Stage 5: assess the risks The risks to information assets are assessed using the risk assessment strategy determined in Stage 3 Each breach of security is assigned a level of risk determined by its likelihood and by its impact on the organisation (Clause 4 2 1(e))

Stage 6: identify and evaluate options for the treatment of risks The risks have their treatment chosen The choices are to accept the risk, avoid the risk, transfer the risk, control the risk A risk is accepted only if it meets the criteria for risk acceptance defined at Stage 3. If the choice is to avoid a risk or transfer a risk (to another organisation, such as an insurer or subcontractor), a suitable means of avoidance or transfer is identified Otherwise the choice is to control (i e lower) the risk

> to the asset (by taking measures to reduce the asset's vulnerabilities), in which case the risk is assigned a priority level for treatment (Clause 4 2 1(f))

Documents generated in the risk assessment task must present evidence that every risk has been assessed, along with a justification for the outcome – acceptance, avoidance, transfer or control – of each individual assessment

5.2.4 Risk treatment

The risk treatment task is again carried out at unit level, in light of polices set out in Stages 1 to 3 The risks treated are those chosen for control at Stage 6.

> **Stage 7: select control objectives and controls** For each risk chosen for control at Stage 6, a suitable control (countermeasure) must be selected from those suggested in the Standard or from elsewhere. The risks are treated in order of priority, according to the priority levels assigned at Stage 6. (Clause 4 2 1(g))

Suitable controls are listed in Annexe A to Part 2 of the Standard, though this list is not exhaustive

Documents drawn up in the risk treatment task should include evidence that each risk has been treated appropriately

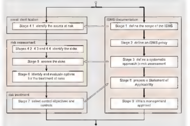

asset identification
Stage 4.1 identify the assets at risk
risk assessment
Stages 4.2, 4.3 and 4.4 identify the risks
Stage 5 assess the risks
Stage 6 identify and evaluate options for the treatment of risks
risk treatment
Stage 7 select control objectives and controls
ISMS documentation
Stage 1 define the scope of the ISMS
Stage 2 define an ISMS policy
Stage 3 define a systematic approach to risk assessment
Stage 8 prepare a Statement of Applicability
Stage 9 obtain management approval

Figure 3 The relationship between the stages and the tasks in the ISMS planning and documentation process

Activity 13

In your own words, describe the tasks and stages of the ISMS planning and documentation process. Clearly identify the stages that are carried out at organisation level from those that are carried out at unit level within an organisation. Identify the information that flows between the tasks/stages.

View discussion

Other approaches to information security

management

Many of the approaches to planning an ISMS to be found in the literature follow a three-phase, rather than a four-task, approach. For instance, Moses (1994) stipulates seven steps in three phases:

- **initiation:** the identification of information assets and their security requirements,
- **analysis:** the identification of possible risks to the security requirements of information assets, of the vulnerabilities to those risks, and of the impact on the organisation of breaches of the security requirements,
- **management:** the identification and justification of countermeasures where needed.

Moses's initiation phase corresponds to our asset identification and his analysis and management phases together correspond to our risk assessment and treatment.

Alberts and Dorofee (2003) specify another three-phase process. Again, the task of the first phase is to identify the organisation's information assets and their security requirements, but it also includes a threat analysis. In Alberts and Dorofee's second phase, the technology systems with which each information asset is associated are determined, so that vulnerabilities to the threats uncovered in the previous phase can be listed and assessed. Each system is then evaluated for the probability and impact of an attack, so that threats and risks can be prioritised. In the third and final phase, the plan comes together with the choice and tailoring of controls.

You will notice that the three-phase approaches of Moses and of Alberts and Dorofee omit the ISMS documentation task. Moreover, neither of these approaches covers the preparation of a Statement of Applicability or the submission of the final set of documents to senior managers for approval. The difference is that, in both cases, the authors focus only on risk analysis and management, and so miss the Standard's requirement for certification of the ISMS. The documents generated in the ISMS documentation task are a major component of what would be delivered to a certifying authority, and provide much of the basis for traceability and for the management of change.

5.3 Setting up an ISMS

Clause 4.1 of Part 1 of the Standard describes the processes and personnel required to support an ISMS under development or in operation. Chapter 4 of *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book) provides a detailed description of each of the components of such support systems, as well as exploring their interrelationships.

Activity 14

Study **Reading 3** (linked below), a short section from Clause 4.1 of Part 1 of the Standard, and Chapter 4 of the Set Book (the subsection of Chapter 4 of the Set Book entitled 'BS 7999 project group' should, of course, read 'BS 7799 project group'). Then summarise the main structures and roles that are suggested by the Standard for an organisation that is developing an ISMS.

Click below to open Reading 3 (0.04 MB).

Reading 3

Guidance

1. Both readings discuss the structures needed to support the development and operation of an ISMS. Although you need to be familiar with these structures, this unit will not require you to develop or implement them.

2. Note that the Standard generally makes *suggestions* for infrastructure rather than laying down requirements. The Set Book, however, describes the systems that would be needed if the suggestions of the Standard were to be accepted *in full*.

3. Unless specified otherwise, the references in the Set Book to clauses of the Standard are to clauses in Part 2 of the Standard. Furthermore, references prefixed by A, B, C or D are to Annexes A, B, C and D of Part 2. The Set Book sometimes refers to clauses in Annexe A as 'controls', since the clauses in that annexe describe the controls specified by the Standard. Note also that the controls in the clauses of Annexe A of Part 2 of the Standard are discussed in more detail in the corresponding clauses of Part 1, so that, for example, the control in clause A.4.1.1 in Annexe A of Part 2 is discussed more fully in clause 4.1.1 of Part 1.

4. The Set Book uses ISO 17799 as a shorthand for what we prefer to refer to as Part 1 of the Standard. Sometimes, particularly when referring to clauses of the Standard, the Set Book uses BS 7799 as a shorthand for what we prefer to call Part 2 of the Standard; at other times, rather more correctly, it uses BS 7799 to refer to complete Standard, both Parts 1 and 2.

5. For the purposes of this activity, you are not expected to read or look up any parts of the Standard other than Clause 4.1 of Part 1. Do not spend time looking up the references

in Chapter 4 of the Set Book to other parts of the Standard You should also ignore suggestions for looking at other chapters of the Set Book

6. ISO 9000, referred to in Chapter 4 of the Set Book, is the International Standard for quality assurance or quality management systems

View discussion

5.4 ISMS documentation

In this subsection we shall consider Stages 1, 2 and 8 of the ISMS documentation task Stage 3 is considered in Section 6 We shall not discuss Stage 9 in this unit

5.4.1 Context, scope and information security policy

An ISMS is defined in Clause 3 4 of Part 2 of the Standard as a

> management system, based on a business nsk approach,
> to establish, implement, operate, monitor, review, maintain
> and improve information secunty

Some organisations will want to protect all of their information assets Others, depending on the business nsks and other hazards they face, may want to consider an ISMS that protects only some of them Examples of organisational units that might need protecting include research and development, payroll, databases and – given their increasing importance and vulnerability – any online operations

As you have seen, this decision on which areas to protect – the question of context and scope – launches the ISMS planning process. By defining the *scope* of the ISMS – which parts of the organisation need its protection – the information assets that need protecting begin to become visible. Defining the *context* of the ISMS – the relationship (business, physical, legal, regulatory, etc.) the protected areas hold to the remainder of the organisation and to the rest of the world – sheds light on the threats that they must be protected against.

The definitions of the scope and context of the ISMS are recorded in the information security policy.

Activity 15

Study **Reading 4** (linked below), an extract from Clause 3.1 of Part 1 of the Standard, and the sections of Chapter 5 of *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book) entitled 'Information security policy' and 'A policy statement'.

Click below to open Reading 4 (0.05 MB).

Reading 4

(a) Describe the personnel who should be involved in the development of an information security policy. Whom should the policy cover?

(b) Describe the possible scopes of an ISMS, and relate these to your organisation.

(c) Consider the role of an ISMS in protecting a *collection* of information assets, and explain how the scope of the ISMS relates to the shareability regions of the assets in such a collection.

(d) Apply the initial policy statement given on pages 64–65 of the Set Book to your own organisation. What can you say at this stage about items (a) and (d)–(f) listed on page 65? (Item (b) is studied in the next section and (c) is outside of the scope of this unit.)

Guidance

Chapter 5 of the Set Book describes Stages 1 and 2 of the ISMS planning process in detail, with references to clauses of the Standard. You are not expected to look up the references to these clauses, or to other chapters of the Set Book, as part of this activity

The reference to '17799' on pages 62 and 65 of the Set Book should of course be to 'ISO 17799', while nearby on both pages 'the standard' refers to Part 2 of the Standard. The unattributed definition of information at the foot of page 62 comes from the Introduction to Part 1 of the Standard

View discussion

5.4.2 The Statement of Applicability

The composition of the Statement of Applicability of the ISMS is Stage 8 of the ISMS planning process

Activity 16

Read the section of Chapter 6 of the Set Book entitled 'Selection of controls and statement of applicability' and then describe the role of the Statement of Applicability. As before, references to 'the standard' mean Part 2 of the Standard.

[View discussion](#)

6 Risk assessment and asset identification

6.1 Introduction

Section 5 discussed the ISMS planning and documentation process in general and also went into the details of Stages 1, 2 and 8 of the ISMS documentation task. In this section, we shall discuss Stage 3 of the ISMS documentation task and see how to define a systematic approach to risk assessment. We shall also look at the asset identification task. The remaining two tasks, risk assessment and risk treatment, are outside the scope of this unit.

6.2 A systematic approach to risk assessment

In Section 4 of this unit you learned of the immense value of information to modern organisations. However, without a storage medium of some kind – paper, a hard disk, a white board, a human memory – information is entirely ephemeral. Once recorded in a medium, though, information endures and can be manipulated, but it also becomes subject to the vulnerabilities of that medium and of the systems that access that medium. And once there are vulnerabilities, there are threats to the security of the information.

In this subsection, we look at how we can develop a systematic approach to assessing the risk of different threats to the security of information assets by analysing the vulnerabilities of the media and systems used to store and manipulate the assets and by estimating the likelihoods of the threats. We shall see how this information can be combined with an evaluation of the impact on an organisation of each security breach to provide a risk assessment for each threat to an information asset.

Activity 17

Study **Reading 5** (linked below), the section from the Introduction to Part 1 of the Standard entitled 'How to establish security requirements'. How does the Standard define risk assessment? What concepts underpin this definition?

Click below to open Reading 5 (0.1 MB).

Reading 5

View discussion

6.2.1 Threats, outcomes and impacts

For the purposes of this unit, we define a *threat* to an information asset as a possible way in which the asset can have its security requirements breached, and we define the *outcome* of a threat as the way in which the asset's security requirements would be breached if the threatened action were to occur. Recall from Section 4 that the security requirements are confidentiality, integrity and availability.

A complete picture of the relationship between an information asset, the threats to it and their outcomes is set out in Figure 4. Figure 4 is adapted from Figure 5-4 of Alberts and Dorofee (2003).

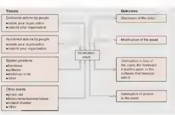

Threats
Deliberate actions by people
• inside your organisation
• outside your organisation
Accidental actions by people
• inside your organisation
• outside your organisation
System problems
• hardware
• software
• malicious code
• other
Other events
• power cut
• telecommunications failure
• natural disaster
• other
Information asset
Outcomes
Disclosure of the asset
Modification of the asset
Destruction or loss of the asset, the hardware it resides upon, or the software that interacts with it
Interruption of access to the asset

Figure 4 The relationship between an information asset, the threats to it and their outcomes

Figure 4 classifies the threats into four types, as follows

- **Deliberate actions by people**, which can come from two groups of persons: those *inside* an organisation and those *outside* it. Examples include a malcontent employee shredding important documents and a hacker attacking a password file. The threats from deliberate actions by people can be further classified into malicious and non-malicious threats.
- **Accidental actions by people**, which again can come from the same two groups: those *inside* and those *outside* an organisation. Examples might be an employee accidentally deleting an important file and a family member spilling coffee on the keyboard of a computer.
- **System problems**, which include: hardware problems (for example, a server crash making the files on a hard disk unrecoverable); software problems (such as bugs, or the system

clock being incorrect and causing a backup program to function incorrectly); and malicious code (maybe a virus or Trojan horse)

- **Other events** include power cuts, telecommunications failures, fire, rodents, meteorites, earthquakes, volcanic eruptions, cosmic rays, and so on. Even severe weather conditions can be a threat to some equipment.

The figure also identifies four possible outcomes for each threat, as follows.

- **Disclosure of the asset**, such as when a hacker releases an online trader's customers' credit card details. In this case, the outcome of the threat is a breach of an information asset's confidentiality requirements.
- **Modification of the asset**, such as a fraudulent increase in the balance of a bank account. Here, the outcome is a breach of an information asset's integrity requirements.
- **Destruction or loss of the asset, the hardware it resides upon, or the software that interacts with it**, such as the loss of an important file due to scratched optical backup media. In this case the outcome is a breach of an information asset's long-term availability requirements.
- **Interruption of access to the asset**, such as a web-server upgrade interrupting online access to an organisation's web services. Here the outcome is a breach of an information asset's short-term availability requirements.

Related to the concept of threat is that of *attack*: a threat is a *way* of breaching the security requirements of an information asset, an attack is an *attempt* to breach them. Any threat could turn into an attack, which could be successful or unsuccessful. An unsuccessful attack has no impact

The *impact* on an organisation of a successful attack on an information asset will depend on how, and to what degree, the organisation's operations are disrupted. For instance, the impact could be measured in terms of the embarrassment caused to the organisation, or its loss of reputation, the harm caused by its being unable to fulfil its mission, lost revenue, wasted investment, or other financial loss, or legal or regulatory liabilities incurred.

The relationship between threat and impact is a simple one: a *threat* has the potential to have an *impact* on an organisation.

Activity 18

(a) Define 'threat' and 'attack' in relation to an information asset.

(b) Distinguish between the 'outcome' of a threat and the 'impact' of an attack.

(c) Describe, with examples, the possible types of threat to an information asset.

(d) Describe the possible outcomes of a threat to an information asset, in each case stating which of the asset's security requirements has been breached.

(e) Read the report entitled 'Top secret military plans found on city dump'. Identify the information asset, the threat to it and the outcome of the threat. What do you think was the impact of the security breach?

View discussion

6.2.2 Threats and vulnerabilities

A hacker who threatens your organisation's information assets is taking advantage of vulnerabilities in the media and systems which handle them. Vulnerabilities and threats clearly go hand-in-hand: each threat is directed at a vulnerability.

The relationship between information assets, threats, vulnerabilities and existing defences is illustrated in Figure 5, which depicts an information asset that is only partially protected by the defences of the media and systems handling it. Some threats will be defeated by these defences, but other threats can take advantage of unprotected vulnerabilities and, in the worst case, compromise the information asset. The aim of an ISMS must be to identify and repair crucial vulnerabilities in media and systems. Figure 5 is adapted from a figure used in a course presented at Stevens Institute of Technology in 2003.

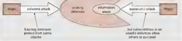

threat
defeated attack
existing defences
information asset
successful attack
threat
Existing defences protect from some attacks
... but vulnerabilities in an asset's defences allow others to succeed

Figure 5 The relationship between information assets, threats, vulnerabilities and existing defences

Activity 19

(a) Define the *vulnerability* of an information asset.

(b) For each of the following situations, describe the information asset, the medium or system which handles it, a possible threat to it, and a possible defence.

(i) a businessman riding his motorcycle to work and mulling over a new business idea;

(ii) a customer withdrawing money from a cash machine outside a bank;

(iii) a contractor digging holes near an organisation's communications cables;

(iv) a poorly trained IT support person working on a company database.

View discussion

6.2.3 Likelihood, impact and risk

Having looked at threats, vulnerabilities, outcomes and impacts, we are now in a position to offer a definition of risk with regard to threats to the information assets of an organisation. This definition will lead to an approach to measuring and assessing risk that is consistent with the Standard and with *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book). This systematic approach to risk assessment corresponds to Stage 3 of the ISMS documentation task in the ISMS planning process.

Parker (1981, p. 141) defines *risk* as 'the product of the amount that may be lost [the *impact*] and the probability of losing it [the *likelihood*]'. Parker here uses the word 'product' in its loosest mathematical sense, i.e. as the combination of two quantities in some way. According to this definition, then, risk comprises two quantities – an impact and a likelihood – combined in some way. As we have seen, the *impact* of a threat is harm done to an organisation if the threat were to turn into a successful attack. The *likelihood* of the threat is the probability that the threat will result in a successful attack

Parker's definition of risk suggests that both the impact and the likelihood could be expressed as numbers. However, estimating numerical values for these quantities is, as you might imagine, fraught with difficulty. Therefore, in this unit, we take the pragmatic, but effective, widely used and respected, *qualitative* approach to risk, in which impact and likelihood can take only three values: low, medium or high. These values are best interpreted in their relation to one another: for instance, a low-impact event will cost the organisation less than a medium-impact event, and a medium-likelihood event will, on average, occur less frequently than a high-likelihood event. However, the ISMS documentation should include some rough-and-ready definition of what 'low', 'medium' and 'high' are to be taken to mean. For example, definitions of levels of impact might be:

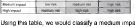
- low impact means 'has negligible effect on the organisation',
- medium impact means 'has considerable effect on the organisation, but the organisation's existence is not threatened',
- high impact means 'the organisation's existence is threatened'.

For likelihood, examples are:

- low likelihood means 'practically never',
- medium likelihood means 'in the order of once a year',
- high likelihood means 'in the order of once a week, or more often'.

The choice of scales for measuring impact and likelihood should be justified by reference to the organisation's objectives and its environment.

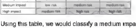
Using these scales, we can combine impact and likelihood to produce a *risk combination table*, which provides a measure of risk One way of doing this is to consider impact and likelihood as being equally important, giving rise to the following risk combination table



	Low likelihood	Medium likelihood	High likelihood
Low impact	low risk	low risk	medium risk
Medium impact	low risk	medium risk	high risk
High impact	medium risk	high risk	high risk

Using this table, we would classify a medium impact, high likelihood threat as of high risk

Another possible risk combination table, which de-emphasises impact, is the following



	Low likelihood	Medium likelihood	High likelihood
Low impact	low risk	low risk	low risk
Medium impact	low risk	medium risk	medium risk
High impact	medium risk	high risk	high risk

Using this table, we would classify a medium impact, high likelihood risk as of medium risk

The final task in defining the organisation's approach to risk is to decide what constitutes an acceptable level of risk If a risk combination table is being used, there are only three possibilities

1. No risks are acceptable: all risks, whether low, medium or high, should be treated
2. Low risks are acceptable: only medium and high risks should be treated
3. Low and medium risks are acceptable: only high risks should be treated

For any organisation, the choice will be based upon several interrelated factors, including the resources (money, personnel, etc) available for implementing the ISMS, past experience of information security breaches, and the maturity of the current ISMS (if there is one). It should also reflect the current approach to risk of other organisations in the same sector. In addition, an organisation's approach to risk may change if new legislation or regulation comes into force, or if new contractual obligations arise.

The approach to risk – the characterisation of impact and likelihood levels, the risk combination table and the acceptable level of risk, together with their justifications – is recorded as part of Stage 3 of the ISMS documentation task in the ISMS planning process.

Activity 20

(a) In Activity 11, you identified an information asset that is valuable to your organisation. In terms of low, medium and high impact, as we interpreted them above, assess the impact that a breach of its security requirements could have on your organisation. What do you think is the likelihood of a breach?

(b) Estimate the impact and likelihood of email being unavailable for (i) one day, (ii) one week, (iii) one month in your organisation.

(c) Estimate the impact and likelihood of secure communications with your customers or clients being unavailable for (i) one day, (ii) one week, (iii) one month in your organisation.

(d) (i) Define a risk combination table that is suitable for an organisation with few resources to allocate to security. What would be an acceptable level of risk for such an organisation?

(ii) For your organisation, define a risk combination table and the level of risk that would be acceptable.

Guidance

In most cases, such as those of (b) and (c), it is difficult to estimate impact and likelihood. The best we can do generally is to act on our gut feeling, informed by experience. The danger of a mistaken evaluation of impact and likelihood is that the wrong risks will be treated, or that some risks will not be treated at all. For the purposes of this unit, however, it is sufficient just to try to make appropriate estimates, to record your decisions and to justify your choices. The experience you gain from this will mean that, if you should ever come to implement an ISMS for real, you will be well aware of the complications that can arise.

View discussion

6.3 Asset identification

You have now completed your study of the ISMS documentation task in the ISMS planning process. In this subsection we study the asset identification task.

You saw in Section 5 that asset identification consists solely of Stage 4.1 of the ISMS planning process, in which the information assets at risk are identified, along with their owners, their locations, their values and their information security requirements. This stage can be subdivided into four steps.

Step 1: identify the boundaries of what is to be protected.

Step 2: identify the information assets, the media in which they are represented and the systems that handle them.

Step 3: identify the relationships between information assets, media, systems and organisational objectives.

Step 4: identify those information assets, media and systems critical to organisational objectives.

These steps are identified on pages 73–74 of *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book).

The definition of the scope of the ISMS, produced in Stage 1 of the ISMS documentation task, is used in Steps 1 and 2, to help identify the boundaries and the information assets.

Step 2 includes the identification of the owners, locations and security requirements of the information assets. The identification of the media and systems allows assets to be grouped according to the storage medium on which they are represented or according to the system(s) that handle them. This grouping of assets aids the execution of Steps 3 and 4 by allowing us to consider together all those assets represented on the same storage medium or handled by the same system(s). This grouping process is helpful not only during asset identification but also during risk assessment and treatment.

It is at Step 3 that the value of an information asset (or group of assets) to an organisation is determined: the greater the asset's contribution to organisational objectives, the greater its value to the organisation. In some circumstances it may be possible to assign a monetary or numerical value to an asset, but in the context of information security it is usually sufficient to classify the value as being low, medium or high (as in the classification of impact, likelihood and risk in the previous subsection). The value assigned to an asset can be useful in determining the impact of a breach of the security requirements of the asset.

The value assigned to an asset (or group of assets) feeds into Step 4 as a factor in determining those assets critical to organisational objectives. The importance of this step is that, in practice, it is unlikely that an organisation will have the resources to protect fully all of its assets In these circumstances, risk assessment and treatment will need to focus on the critical assets, at least to begin with, other, non-critical assets can be protected later, if resources allow At this step, it can often be useful to rank assets in an order of priority for risk assessment and treatment determined by how critical they are to organisational objectives.

Activity 21

Read the subsections of Chapter 6 of *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book) entitled 'Identify the boundaries', 'Identify the systems' and 'Identify relationships between systems and objectives' (pp 74–76) As you read, relate the Set Book's discussion of the asset identification task to the four steps described above

(a) (i) Define the smallest practicable scope for which an ISMS can be developed

> (ii) State one criterion for deciding whether one or many ISMSs should be implemented
>
> (iii) State the defining characteristics of the scope of an ISMS

(b) (i) Use your answer to (a) to help you determine a unit within your organisation to which a single ISMS should be applied You should aim to choose a unit within which you work

> (ii) Give examples of two or more of the systems for handling information assets within the unit you identified in (b)(i), preferably ones that you use on a daily basis By consulting within the unit, identify the critical assets that

rely on these systems

(c) Explain why

(i) information assets and organisational objectives need to be related,

(ii) information assets need to be prioritised

Guidance

1. The Set Book uses the term 'organisation' ambiguously, both to refer to a large entity consisting of many units, often at different premises, and to a unit within such an entity We endeavour in the main text of this unit to restrict the use of organisation to the large entity and to use the term 'unit' for a part of the large entity to which an ISMS is to be applied Of course, in some cases we wish to apply an ISMS to the whole of a large entity, in which case the meaning of the terms 'organisation' and 'unit' coincide
2. To help you determine the scope of an ISMS within your organisation, so that you can answer (b)(i), you might like to draw a diagram showing the structure of your organisation, how information is shared across unit boundaries, units with a common culture, and so on

View discussion

The asset identification process described above is one of many in the literature Others include the following

- Parker (1981), one of the earliest books to discuss information security (which he calls 'computing security'), provides excellent practical guidance on identifying assets in Chapter 9

- Alberts and Dorofee (2003) have developed what they call the OCTAVE approach to managing information security. It includes a full asset identification process.

7 The PDCA cycle

In Section 5 you were introduced to the nine-stage ISMS planning process advocated by the Standard. You have also, in Sections 5 and 6, looked in some detail at some of these stages – those comprising the ISMS documentation and asset identification tasks.

However, an ISMS must not only be planned, it must also be implemented, operated, monitored, reviewed, maintained and improved. Part 2 of the Standard provides guidance on these processes, which it suggests should be undertaken following a *Plan–Do–Check–Act* (PDCA) cycle. Here we introduce you to the PDCA cycle.

Walter Shewhart, a statistician working at Bell Laboratories in the 1930s, is credited with inventing the PDCA cycle. The PDCA cycle is the Standard's proposed methodology for the commission and continuous improvement of an ISMS. The PDCA cycle is also known as the Denning cycle, after the quality management guru W Edwards Denning.

Central to the PDCA cycle is the simple idea that we learn by doing. In the context of tackling a particular problem, the PDCA cycle relates to the idea that the act of building a solution to a problem leads to a better understanding of that problem, which can in turn lead to building a new and better solution, and so on. In its generic form, the PDCA cycle consists of the four iterated stages – Plan, Do, Check and Act – shown in Figure 7.

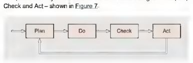


Figure 7 The PDCA cycle

The purpose of the **Plan** stage is to understand the problem and develop an initial, but fit-for-purpose, solution that can be created relatively quickly. Criteria against which the effectiveness of the initial and future solutions can be gauged are also agreed.

In the **Do** stage, the results of the Plan stage are implemented and then used. In the first iteration, this generally just means a pilot study to test the initial solution, so limiting any damage from mistakes in the Plan stage.

In the **Check** stage, the solution is observed in operation. The idea is to answer the following sorts of questions.

- Does the solution work in the way it was expected to? How well does it stand up against the evaluation criteria set up in the Plan stage?
- Has producing a solution changed our perception of the problem? Which parts of the problem do we understand well, and which parts not so well?
- How could we change the solution to make it better? What changes would reflect our new perception of the problem? Which parts of the solution work well and which work poorly?

The answers to questions like these prepare for the **Act** stage, in which the current solution and the results of the Check stage are used to define a revised problem for initiating the Plan stage of the next iteration.

Although not appropriate for all types of problem, the PDCA cycle does provide a way of tackling those problems:

- that exist in a complex and changing environment;

- that need an initial solution relatively quickly,
- for which there exist resources for continual improvement.

These characteristics certainly ought to apply to information security management.

Activity 22

(a) Describe one or more areas of your life in which you use or could use the PDCA cycle.

(b) Identify problems in your own organisation for which the PDCA cycle might be a useful strategy.

Guidance

In tackling both parts of this activity, you may wish to consider the three characteristics of problems to which the PDCA cycle is suited – complex and changing environment, quick initial solution, resources for continual improvement – and assess whether they apply to any part of your work or home life. There may already be daily situations in which you unknowingly apply the PDCA cycle.

View discussion

The PDCA cycle is a significant tool in an organisation's work on information security management. However, it is beyond the scope of this unit to discuss how it can be applied to ISMS management.

8 Summary

This unit has discussed the importance of information assets to any modern organisation and has made the case for information security management. It has introduced you to extracts from the British Standard on Information Security Management and to the approach advocated in the Standard for establishing and managing an information security management system (ISMS). It has also introduced the PDCA cycle. A particular focus in this unit has been on the planning of an ISMS, and on the four tasks and nine stages in this process. The unit has considered in some detail the ISMS documentation and asset identification tasks

References

Alberts, Christopher and Dorofee, Audrey (2003) *Managing Information Security Risks: The OCTAVE Approach*, Addison-Wesley.

Grant, Robert M (1998) *Contemporary Strategy Analysis* (3rd edn), Blackwell.

Itami, H and Roehl, T (1987) *Mobilizing Invisible Assets*, Harvard University Press.

Moses, Robin (1992) 'Risk analysis and management', Chapter 21 in Jackson, K M and Hruska, J, *Computer Security Reference Book*, Butterworth-Heinemann.

Parker, Donn B (1981) *Computer Security Management*, Reston.

Turnbull, Nigel (2003) 'Foreword' in Calder, Alan and Watkins, Steve, *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799* (2nd edn), Kogan Page (Set Book).

Acknowledgements

The content acknowledged below is Proprietary (see terms and conditions). This content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 2.0 Licence

Grateful acknowledgement is made to the following sources for permission:

Figures

Figure 4 Alberts, C and Dorofee, A (2002) *Managing Information Security Risks: The OCTAVE Approach*, Addison-Wesley, adapted by permission;

Figure 5 McNair, B (2003) *Security Topics: How Much Security Is Enough?*, copyright © Stevens Institute of Technology, adapted by permission.

Unit Image

Luke Gattuso: Flickr.com [Details correct as of 21 April 2008]

Don't miss out:

Discussion

(a) The mission of the Open University is to be:

- **open as to people** – making university study available to an increasingly large and diverse student body and providing learning opportunities that meet individuals' lifelong needs,
- **open as to places** – providing learning opportunities in the home, workplace and community throughout the UK and selectively elsewhere, and serving an increasingly mobile population,
- **open as to methods** – using and developing the most effective media and technologies for learning, teaching and assessment whilst attaching central importance to the personal academic support given to students, and working collaboratively with others to extend and enrich lifelong learning,
- **open as to ideas** – developing a vibrant academic community that reflects and supports the diversity of intellectual interests of all our students and staff and that is dedicated to the advancement and sharing of knowledge through research and scholarship.

(b) Within the Open University there are very many types of information that are required to meet this mission. Examples include the following.

- **Teaching information** This information is provided in the huge range of courses the OU produces, thus supporting the first, third and fourth of the mission statements. By providing teaching information in a variety of formats, including printed text and electronic text, the second mission statement is supported too.

- **Research information** This information is embodied in the research documents written by OU researchers, and supports the third and fourth mission statements

  The teaching and research information also provides the basis for much of the OU's funding, thus indirectly supporting all four mission statements

- **Administrative Information** An example is provided by the student records kept on courses studied and results, one use of which is to allow the OU to suggest appropriate choices of future study, thus supporting the first mission statement.

- **Strategic information** Such information includes documents that explore the possible futures of the OU, including proposed buildings, academic programmes and catering plans, thus providing support for all the mission statements

The openness expressed in the mission makes the value of information difficult to preserve, and so this openness needs to be tempered by some measure of **closedness**, to protect the OU's competitive advantage in teaching, for instance.

(c) The Introduction to *IT Governance A Manager's Guide to Data Security & BS 7799/ISO 177799* stresses the 'convergence between business management and IT management' and hence the importance of information in the running of a business It also asserts that the 'commercial viability and profitability' of organisations 'increasingly depends on the security, confidentiality and integrity of their information' Later, it states that information is becoming 'more and more the strategic [enabler] of organisational activity' and that it is 'the very life-blood of most organisations today'

Back

Discussion

(a) The three reasons are:

1. organisations working in a high-technology environment depend more and more on their information systems;
2. the public is increasingly concerned about the proper use of information;
3. threats to information systems from criminals and terrorists are increasing.

(b) You may consider that one or more of the three reasons given in the answer to (a) applies to your organisation, in which case your studies in this unit may be an attempt (by you or your organisation) to learn more about information security. Professional thinking about information security and its management – the focus of this unit – may help your organisation assess potential threats to its valuable information. And thinking about the information that is important to your organisation will raise awareness of the value that resides there, and start the important process of protecting that value.

Back

Discussion

1. Information security is characterised as the preservation of the confidentiality, integrity and availability of information.
2. According to the Standard, information security is achieved by choosing and implementing a set of controls – these could be policies, practices, procedures, organisational structures or software functions – to ensure that the information security objectives of the organisation are met.

Back

Discussion

Here are some of our thoughts.

- We wondered about the extent to which expressions such as 'flood of threats', 'web of legislation', 'clear and present danger', 'random unprovoked attacks', 'no organisation is immune', 'every organisation will suffer' might have been chosen to resonate with (or even exploit) today's social and political anxieties.
- We noticed that some of the surveys and opinions cited come from parties who may have an interest in promoting the information security industry. Management consultants market expertise in this area, enforcement agencies have to make the case for budgets and resources for new areas of activity, the UK government (DTI) promotes the interests of UK businesses internationally, including security and IT businesses.
- We felt that most of the statistics raised more questions than they answered. Many of them suggest more research is needed to understand more clearly the nature and scale of threats. The measurement scales for many of the reported results were unclear, and there are obvious difficulties in costing security breaches, including some of the most common. Here are some specific examples of what we mean.
  - Compare 'European businesses ... lost £4.3 billion in [2000] due to Internet-related crime' (p. 11) with 'in 2001 ... the annual cost to the German economy of deficient IT security was higher than £96.3 billion' (p. 12).
  - The statement that '69% recognised that they possessed information that was either sensitive or critical' (p. 9) leaves open several important questions, such as what volumes of

such data were held and how exposed it was. Nor is it clear what portion of the measurement scale is covered by the classes 'sensitive' to 'critical'.

- We noted (from p. 9) that 63% of the 69% cited (i.e. 43% of those surveyed) had suffered a moderately serious breach or worse. We are not told what portion of the measurement scale is covered by the class 'moderately serious breach or worse'.
- The increase of virus incidents from 20% to 73% (reported on p. 11) deserves exploration. Was it just one virus, or many, that infected many organisations?
- The authors offer a variety of figures assessing the 'average cost' of security breaches, e.g. 'the cost of a single breach was in excess of £100,000' (p. 10), 'the average cost of serious security incidents was £30K' (p. 10), 'average losses … in the order of $2 million' (p. 12). Information on whether these were the mean, median or modal costs would be valuable. Furthermore, information on the distribution of costs would help.
- If 90% of organisations suffered a malware attack, but 80% of these had antivirus software (reported on p. 13), then we need to know whether or not antivirus defences are effective.
- We learn that 'insider security incidents occurred more often than outsider ones' (p. 13), but that these incidents included installation of unauthorised software, unauthorised email, gambling, pornography, personal businesses. Do these activities really pose a threat?

- Given its focus on IT governance, the Set Book naturally concentrates on threats to computer-based communication and storage. However, it is worth remembering that the more traditional form of industrial espionage, in which physical documents and plans are acquired, is still widely practised and is still a threat not to be underestimated.

Back

Discussion

Here are some examples in the case of the Open University.

Law	Example
Data Protection Act 1998	Relevance to OU: governs the storage and use of information about staff and students.
	Effect: the University is careful to communicate its policy to staff and students and to monitor internal compliance.
Freedom of Information Act 2000	Relevance to OU: establishes the public's right of access to information relating to policy, decision-making and use of public funds by the University.
	Effect: the University has systems to ensure that relevant information is either publicly available (e.g. in the OU Library) or appropriately archived.
Computer Misuse Act 1990	Relevance to OU: protects the University's computer systems from unauthorised access.
	Effect: the University has systems for monitoring potential abuse.
Copyright Designs and Patents Act 1988	Relevance to OU: protects the rights of the University with regard to its published materials.
	Effect: all materials associated with this and other courses are copyrighted.
Electronic Communications	Relevance to OU: limits the cryptographic protocols that can be used by the University

Act 2000	
	Effect: restricts the protocols used by staff for remote computer access.
Human Rights Act 1998	Relevance to OU: the University affects the lives of people
	Effect: regulates the activities of the University among the communities within which it works.
Regulation of Investigatory Powers Act 2000	Relevance to OU: the University uses much electronic communication and has many employees.
	Effect: gives the University an assurance that its electronic communication cannot be unlawfully intercepted and limits the University's power to monitor staff activity
Public Interest Disclosure Act 1998	Relevance to OU: the University is an employer.
	Effect: the University has a 'whistle-blowing' procedure which guides employees in what to do if they believe the University has engaged, or intends to engage, in criminal or civil wrongdoing.

Back

Discussion

(a) We identified the following imperatives. The page references in the table are to the Set Book

Type of organisation	Imperative
publicly listed company (plc)	Combined Code and Turnbull Report (pp 19–21)
organisation in supply-chain relation with a plc	Indirect pressure of Combined Code and Turnbull Report (pp 21–22)
UK Government (HMG)	Turnbull adapted as Orange Book (p. 22)
non-governmental organisation (NGO)	Turnbull adapted as Orange Book (p. 22)
non-departmental government body (NDPB)	Turnbull adapted as Orange Book (p. 22)
organisation in supply-chain relation with HMG, NGO, NDPB	Indirect pressure of Orange Book (p. 22)

The extent to which supply-chain organisations need to comply with the Combined Code, Turnbull Report or Orange Book is currently unclear. However, the more an organisation is able to demonstrate compliance with these imperatives, the fewer are the barriers to its participation in a supply chain.

(b) The Open University receives funding from the Government via the Higher Education Funding Council for England and Wales (HEFCE). Following Turnbull, HEFCE published guidance on internal control and risk management for university governing bodies and senior managers

Back

Discussion

A practical definition of 'ethical conduct', based on the effect of our conduct on others, is proposed by the OECD: ethical conduct is behaviour that respects the legitimate interests of others.

This understanding of ethical conduct based on the duties to others is also evident in many published codes of professional conduct. For example:

- The Institute of Directors publishes a Code of Professional Conduct for Chartered Directors. The fourth article of the code requires that a chartered director shall 'exercise responsibilities to employees, customers, suppliers and other relevant stakeholders, including the wider community'.
- The Chartered Management Institute invites members to reflect on how they might rate as an ethical manager. Among other questions, managers are asked whether they 'take account of whether actions seem right and fair, or whether they are hurting anyone's interests'.
- The British Computer Society's Code of Conduct maintains that members shall 'have regard for the public health, safety and environment', shall 'have regard to the legitimate interests of third parties' and shall conduct their professional activities 'without discrimination against clients or colleagues'.

Back

Discussion

We identified the following benefits for the Open University.

- As a public-sector organisation, tha OU must meet students' expectations of continuity, confidentiality and privacy of information. Taking information security seriously helps the OU fulfil its obligations to its wider community
- If the OU can demonstrate that it takes information security seriously, this may help it to foster academic and commercial relationships with other organisations that give priority to information security. For instance, in research relationships with commercial organisations, the OU would be given access to commercially sensitive information, such as business rules, critical systems, etc. The ability of the OU to taka information security seriously means that such partnerships are easier to establish, and will endure.

Back

Discussion

(a) (i) As well as its expertise in the soft drinks industry, Coca-Cola owns the recipe for Coca-Cola, and this information could be the source of much of its competitive advantage and value – the recipe is certainly a well-guarded secret

(ii) As well as knowledge and expertise in developing softwere, Microsoft owns Information in the form of the hundreds of millions of lines of code that comprise its software systems, such as Windows and the Office Suite These are an obvious repository of value *Note* While this unit was in production, tens of millions of lines of Microsoft code were released onto the internet One industry commentator remarked that it is now possible that Microsoft's competitors can gain insights into the inner workings of Windows that will allow them to compete more effectively

(b) This is a very difficult question to answer well unless you are systematic The Open University, for example, is involved in many areas of endeavour, including teaching, research, administration, external accreditation and providing advice, and each draws on important information Moreover, how does one *measure* the value of the information?

Back

Discussion

(a) I have installed, and update regularly, an antivirus package, trusting that the package does what it says and stops all forms of malware. I have also installed an application supervisor that allows me to audit outgoing connections from my machine to the internet: any application that asks the operating system to contact another host on the internet has to wait while the supervisor asks me to verify the connection.

(b) I *hope* that this is enough to protect me from the worst forms of spyware. However, there are less insidious, but still invasive, forms of spyware. If you have ever connected to the internet using any computer with a browser, it is almost certain that your internet activities have been tracked by advertising companies by means of *cookies*, pieces of software that record which websites you visit.

The Open University uses a popular, regularly updated antivirus package. It does not *specifically* protect against spyware, though. Nor is there any policy on the use of cookies: in fact, internally, cookies *are* used to track the OU's use of resources.

Back

Discussion

(a) The Open University's mission includes using the most effective technologies for learning, teaching and assessment. It gains its competitive advantage (within the university sector) in this regard through its model of teaching at a distance, which is partly based on tutor-marked assignments, or TMAs. Tutor Notes are marking schemes that guide tutors in how to mark TMAs accurately and consistently, and so are important information assets for the OU.

(b) Tutor Notes need to be *shareable* between the course team (who prepare them), the external examiner (who assesses them) and the tutors (who mark from them). They also have to be edited and printed, so other OU employees and systems will require access to them too. But, for obvious reasons, Tutor Notes must be scarce outside this region: they should not be available to students or appear on any system outside the OU in a recognisable or understandable form.

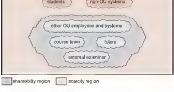


Figure 1 The shareability and scarcity regions for the Tutor Notes for an OU course

(c) The regions should not overlap, or else any system or person in the intersection could potentially act as a channel along which the information asset could flow into its scarcity region. In the case of the shareability region for the Tutor Notes, however, there is a potential overlap if an OU employee who would normally have access to Tutor Notes is also an OU student; this is overcome by strict regulations stipulating that the shareability region for a course's Tutor Notes explicitly excludes members of staff who are studying that course.

The shareability region for Tutor Notes does not correspond to a recognisable unit of activity in the OU. In many cases, however, the shareability region does correspond to a recognisable unit of activity within an organisation.

(d) An organisation needs to have control over the whole of the shareability region of each information asset. In theory, those parts of a shareability region that comprise the organisation's systems and personnel ought automatically to be under the organisation's control. If parts of a shareability region extend beyond the organisation, control will be harder to exert.

An organisation is likely to have little or no control over the scarcity region of an information asset. The wider world is a wild and ungovernable place!

Back

Discussion

(a) To meet the shareability goal, the information asset should be available and have full integrity within its shareability region.

To meet the scarcity goal, the information asset should be kept confidential within its shareability region or, if the information asset must be made available within its scarcity region, the integrity of the asset should be destroyed or reduced as it is moved into its scarcity region.

(b) These are requirements specific to information assets, so they do not apply to non-information assets. You may like to discuss the security requirements for non-information assets with other learners, using the Comments section below.

(c) For Open University Tutor Notes, our assessment is as follows:

- If the Tutor Notes were disclosed to students, they would no longer serve their purpose, and so their value would be reduced. Therefore Tutor Notes are subject to the confidentiality requirement.
- If the Tutor Notes were corrupted, this would interfere with the marking of students' work, and so their value would be reduced. Therefore Tutor Notes are subject to the integrity requirement.
- If the Tutor Notes were unavailable to tutors, then they would have no value in students' assessment. Therefore Tutor Notes are subject to the availability requirement.

You may have found that your information asset was similar, or subject to only one or two information security requirements.

(d) As a different example, we consider a scenario close to all students' hearts. When teaching and assessment of an OU course is complete, an Examination Board meets to consider the marks for each and every student The marks are presented in the form of a number of computer-generated tables, along with detailed statistical analyses to help the Board interpret the results of individual students and those of the whole cohort

- Availability is particularly sensitive to timing If the cohort marks were unavailable for only one hour, say, this would probably have no appreciable adverse affect However, if they were not available for a day or a week, this would create considerable problems for the Board members, who would have to rearrange appointments to attend a rescheduled Board, and there would probably be knock-on effects on other boards, though students would be unlikely to experience any impact at all However, total loss of the data would be an altogether different matter students would need to be reassessed and the reputation of the Open University could be seriously undermined
- Lack of integrity of the data would have a particularly damaging effect if it only came to light after results letters were sent to students If the Board's procedures detected the problem, the impact would be comparable to a delay in availability
- A breach of confidentiality before the official announcement of results could severely damage the reputation of the OU If the breach related to an identifiable student, the OU might reasonably expect legal action

(e) The possible results of a breach of information security are a reduction in confidentiality, a reduction in integrity and/or a reduction in availability

Back

Discussion

The activities of the *ISMS documentation* task are to define and record the context, scope and components of the ISMS. It comprises five stages:

- define the scope of the ISMS
- define an ISMS policy
- define a systematic approach to risk assessment
- prepare a Statement of Applicability
- obtain management approval.

These stages are all carried out at the organisation level.

The ISMS documentation task runs in parallel with the asset identification, risk assessment and risk treatment tasks, all of which are carried out at the level of individual organisational units.

In the *asset identification* task, the organisation's information assets, their owners, their locations, their values and their security requirements are established.

In the *risk assessment* task, the risks to those assets are determined, along with the potential costs of breaches of their security requirements. It consists of the following stages:

- identify the risks
- assess the risks
- identify and evaluate options for the treatment of risks.

In the *risk treatment* task, suitable controls are selected to protect the information assets against loss or damage. It consists of a single stage:

- select control objectives and controls

The following information flows between the tasks/stages:

- the scope of the ISMS is used as the foundation for asset identification;
- the ISMS policy and a systematic approach to risk assessment form the starting point of risk assessment;
- the information required to complete the Statement of Applicability is provided by the risk treatment

Back

Discussion

Part 1 of the Standard (Clause 4.1) describes the processes and personnel required to support an ISMS under development or in operation. The main structures and roles that are suggested by the Standard for an organisation that is developing an ISMS may be summarised as follows.

- There should be a *management information security forum*, the role of which is to provide clear direction and visible management support for the ISMS. The forum would be responsible for reviewing and approving information security policy and high-level responsibilities, ensuring sufficient resources for the development, implementation, operation and maintenance of the ISMS, monitoring significant changes in threats to the organisation's information assets, reviewing information security incidents within the organisation, approving initiatives to improve information security, regular reviewing of the ISMS, and allocating information security responsibilities.
- There should be a single *information security manager* responsible for all aspects of information security, including the implementation of the management information security forum's decisions.
- There should be an *authorisation process for new information processing facilities* that will allow the organisation to adopt new technologies without compromising security.
- There should be an *information security adviser*, whose job is to provide advice on specialist topics, including the choice of security technologies required by the ISMS.
- There should be an *independent internal review board* for the ISMS.

Chapter 4 of *IT Governance. A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book) provides a detailed description of each of the components of such support systems, as well as exploring their interrelationships

Back

Discussion

(a) The Set Book identifies the following people as being involved in developing an information security policy: the manager charged with leading the ISMS implementation, the board and management of the organisation, the management information security forum.

The policy should cover all employees in the organisation, or relevant part of the organisation, and may also apply to 'customers, suppliers, shareholders and other third parties' (Set Book, p. 61) – in fact, all those identified in the context of the policy.

(b) The Set Book states that the scope of an ISMS could be determined 'on the basis of corporate [organisational], divisional or management structure, or on the basis of geographic location' (p. 61). It also states (pp. 61–62) that a policy that encompasses all of the activities of a functional unit is easier to implement than one that applies only to a part.

Applying these ideas to the case of the Open University, we might consider a number of alternative scopes, determined:

- by geographic location: the ISMS would apply, for example, to a single regional office, or to the central campus;
- by management structure: the ISMS would apply, for example, to all academic units, or to all IT functions;
- by organisational structure: the ISMS would apply, for example, to an individual faculty, to student services, to IT support, etc;
- by organisation: the ISMS would apply to the whole of the OU.

(c) For a collection of information assets, each of which has its own shareability region, the scope of the ISMS should be larger than, or at least coincident with, the union of the shareability regions of the assets.

(d) For the Open University, the initial policy statement might read:

> The Senate and management of the Open University are committed to preserving the confidentiality, integrity and availability of all the information assets of the organisation in order to maintain its competitive advantage, legal and contractual compliance, image, and reputation. All employees of the organisation are required to comply with this policy and with the ISMS that implements this policy. Certain third parties, defined in the ISMS, will also be required to comply with it. This policy will be reviewed when necessary, and at least annually.

Item (a) would require a statement on the structures and roles relating to the ISMS, as summarised in Subsection 5.3.

The following simple statement covers items (d), (e) and (f) in the case of the Open University:

> The Senate and management of the Open University are committed to the inclusion of information security in the University's mission and business objectives, and to the continuous improvement of information security provisions as the business environment changes. All staff will receive security awareness training appropriate to their role. The University is committed to comply with, and achieve certification to, BS 7799.

Back

Discussion

The Statement of Applicability formally documents the decisions reached on which control objectives and controls have been chosen and which have not, together with the reasons for each decision.

Back

Discussion

The extract defines the notion of *risk assessment* for information security assets as the process in which 'threats to assets are identified, vulnerability to and likelihood of occurrence [are] evaluated and potential impact is estimated'. So risk assessment is defined in terms of the concepts of *threat*, *vulnerability*, *likelihood* and *impact*.

Back

Discussion

(a) A threat is a possible way in which an information asset can have its security requirements breached. An attack is an attempt to breach the security requirements of an asset.

(b) The outcome of a threat is the way in which the security requirements of an information asset would be breached if the threatened action were to occur. The impact of an attack is the cost to the organisation, in terms of financial loss, loss of reputation, etc. of the breach of an information asset's security requirements.

(c) The types of threat are:

- **deliberate actions by people**: examples include writing and distributing a virus and pasting your password on your computer screen,
- **accidental actions by people**: a common example of this is dropping a portable computer,
- **system problems**: an example is a word processor crashing and corrupting an important document,
- **other events**: examples include a fire or flood in a server room.

(d) The possible outcomes are:

- the **disclosure of the asset**, leading to a breach of confidentiality,
- the **modification of the asset**, giving rise to a breach of integrity,
- the **destruction or loss of the asset, the hardware it resides upon, or the software that interacts with it**, leading to a breach of availability,
- the **interruption of access to the asset**, giving rise to a breach of availability.

(e) The information asset consisted of secret ground plans to military installations in Cyprus. The threat is the disposal of these plans as ordinary rubbish, which is probably a deliberate action by someone inside the military. The outcome is the disclosure of the physical documents, presumably in breach of their confidentiality requirements. The impact is difficult to assess, but certainly included embarrassment and loss of reputation, and may even have had much more serious effects, such as making critical information available to hostile groups.

Back

Discussion

(a) A vulnerability is a weakness in the defences of an information asset

(b) We thought of the following answers.

(i) The information asset is the new business idea, the medium is the businessman's memory, and the obvious threat is the businessman being hurt in a motorcycling accident. One possible defence against the threat would be a helmet; a policy of committing new ideas to paper would be a better safeguard.

(ii) The information asset is the customer's PIN, the medium is the keyboard used to enter the PIN into the cash machine, and one threat is that someone will see the PIN being entered. Possible defence includes shielding the keyboard from observers.

(iii) The information asset comprises the data that pass through the cables, the medium is the cables themselves, and a threat is the cutting of the cable. Possible defence includes the armour-shielding of cables and better maps of cable runs.

(iv) The asset is the information in the database, the system is the database itself, and a threat is that the employee's lack of training will lead to some sort of damage to the database, compromising the information it contains. One obvious defence would be to improve the IT support person's training.

Back

Discussion

(a) As in Activity 11, we select the Open University as the organisation on which to base our discussion and Tutor Notes as the information asset

We believe that a wide-scale breach of confidentiality could result in the OU being unable to rely on the results of the TMAs to which the Tutor Notes pertain. Worse, if it took a long time for the breach in confidentiality to be detected, the OU might even have to withdraw course awards, leading to terrible publicity and even legal action Although this could have a severe effect on the OU, we judge it unlikely to threaten the OU's existence, and so we would rate it as medium impact. Tutor Notes are indeed recognised as valuable, and so are protected by a security system. The likelihood of a breach of their confidentiality is, therefore, low.

Damage to the integrity of Tutor Notes would mean only that they would need correcting, and so we think this is a low-impact risk, which is also of low likelihood since great vigilance is required from those involved in their production.

A reduction in availability could result in an inability to mark TMAs and make awards. So we would rate it, like confidentiality, as of medium impact but low likelihood.

The OU is a not-for-profit institution. If your organisation is for-profit, the situation may be very different. For instance, a breach in the confidentiality of a tender (at the wrong time) might certainly threaten the organisation's existence, and so would be of high impact. Its likelihood might well be high also, as competitors may actively be seeking this information

(b) We base discussion on the Open University and the members of the M886 Course Team.

(i) Many of us feel that if email were unavailable for one day this might actually improve our work situation (We would all welcome a short period in which the email torrent dried up.) Consequently, the impact of a short period of its loss would be low. In fact, our mail server does go down from time to time, and it may take a day or so to transfer information to a replacement system. This happens about once a year, on average, so the threat is of medium likelihood

(ii) However, we do use email extensively for arranging meetings, exchanging documents and external communications at short notice If the system was unavailable for one week, then we would have to fall back on old-fashioned means of communication. Nevertheless, it would take a period of many weeks' interruption to disrupt our work in any serious way, so one week's absence of service would probably be of low impact And the absence of email for a week could only happen if there was a catastrophic failure in the OU's mail system, with no replacement available This is of low likelihood

(iii) We rely on email to help us meet our deadlines, such as for the submission of external funding bids and the organisation of consortia, which are major sources of research funding For email to be unavailable for one month or longer could, if this period coincided with a number of such important cut-off dates, have severe consequences for the research finances of academic units. In the worst case, then, this is a medium-impact threat Although it is unthinkable that *all* email could be unavailable for a year, and is therefore of low likelihood, we have found that, quite regularly, *single* messages can go astray, only reappearing months later So we estimate the risk of long-term loss of important messages as being of high likelihood Recent experience of internet service providers marking genuine business email as spam has convinced us that this could occur often.

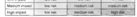
(c) We base this discussion on the case of secure electronic communication between students and the OU handled by the eTMA system.

(i) Loss of the eTMA system for one day around the time of a course deadline could certainly inconvenience all students on that course. However, without wishing to trivialise this inconvenience, we think a single occurrence would have low impact. We asked the developers and maintainers of the eTMA systems about the likelihood of the system becoming unavailable: it is quite possible, we were told, but it hasn't occurred yet. Therefore, we would assess the risk as of medium likelihood.

(ii) If the eTMA system were unavailable for one week at the time of a deadline, it would have a considerable effect on the business of the OU: students' personal timetables would be badly disrupted, and this would in turn affect the work that tutors have to do. In the worst case, confidence in the eTMA system could be damaged, as could the reputation of the OU. The impact of such a failure would thus be medium, but the likelihood of it is low.

(iii) If the eTMA system were unavailable for one month, many courses would have their assessment timetables badly disrupted and thousands of students would have their plans dislocated. Depending on the quality of the OU's backup plans, the reputation of the OU could be severely damaged, perhaps (if it happened more than once) even putting into doubt the future of the institution itself. Without doubt, this is a high-impact threat, but, again, it is of low likelihood.

(d) (i) A cash-strapped organisation will need to focus on the high risks, so that low and medium risks are acceptable It should also classify as high risk only those threats of high impact *and* high likelihood One possible risk combination table is the following



	Low likelihood	Medium likelihood	High likelihood
Low impact	low risk	low risk	low risk
Medium impact	low risk	medium risk	medium risk
High impact	low risk	medium risk	high risk

Any table in which the only high-risk threats are those of high impact and high likelihood would be suitable

(ii) To define the risk combination table and the acceptable level of risk, you should have considered the availability of resources for ISMS development and your organisation's attitude to risk

Back

Discussion

The first of the subsections, 'Identify the boundaries', corresponds to Step 1. The second, 'Identify the systems', corresponds to Step 2. The third subsection, 'Identify relationships between systems and objectives', relates to Steps 3 and 4.

(a) (i) The smallest practicable scope for an ISMS is defined by a boundary across which there is little information sharing, i.e. it is self-contained.

(ii) A single ISMS is indicated when an organisation shares a single business culture and generally uses the same systems throughout. Otherwise, multiple ISMSs should be considered.

(iii) The defining characteristics of the scope of an ISMS for a unit within an organisation are the premises the unit occupies, its network assets and its information assets.

(b) We use the Open University as our exemplar.

(i) Figure 6 is a diagram showing how the Computing Department, to which many of the members of the M886 Course Team belong, fits into the structure of the OU. The arrows indicate the flow of information across boundaries (the breadth of an arrow represents the quantity of information that is shared).

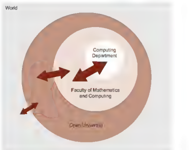


Figure 6

The OU has a large number of premises across the UK, and although some network and information assets are shared there are many that are not. This suggests that the OU as a whole is inappropriate for a single ISMS. Furthermore, the information flows between the Computing Department and the Faculty of Mathematics and Computing are too large for it to be sensible to restrict the ISMS to the Computing Department.

The Faculty of Mathematics and Computing occupies a single building. Networking services, many systems and much information are shared across the Faculty, and there is reasonable common culture throughout the Faculty. The information flows between the Faculty and the OU generally are rather large, but, given that all the other indicators are satisfied, the Faculty is probably a sensible unit to which a single ISMS should be applied.

(ii) Systems that handle information assets and that are used regularly by members of the Faculty of Mathematics and Computing include email, swipe cards, proxy servers, a web server, file servers and internal mail. Course texts, critical to our mission, are held on file servers and exchanged by email.

(c) (i) Breaches of the security requirements of information assets that contribute most to an organisation's objectives will have the greatest impact on the organisation's ability to discharge its mission.

(ii) It may not be possible to protect all information assets, or the protection may need to be phased, so those judged most significant and the most vulnerable must be given priority.

Back

Discussion

(a) One M886 Course Team member thought of the following two examples.

- It would seem that I structure my work day using the PDCA cycle. The day starts with an initial to-do list (Plan), working through the list (Do), I complete tasks, I observe that the list grows and shrinks as new tasks come in, and existing ones are finished (Check). I alter priorities in the list (Act) to accommodate the day's unfolding requirements. Each day, therefore, consists of one or more iterations of the PDCA cycle.
- Software development is an example of the PDCA cycle in action: an alpha release is an initial solution to a problem, which will be internally tried out, tested and changed to complete one PDCA cycle. Then a beta version is released to the wider world and the second iteration begins. Beta testers continue using the software, noting and feeding back problems to the developers, over many PDCA cycles. Later beta versions become candidate final releases, and then final versions are sold to the public. Nor is that the end of the matter, of course: as soon as a final release is in wide circulation, customers send in bug reports which drive further iterations of the PDCA cycle.

(b) The Open University is feeling competition – for the first time – in its provision of university degrees by distance learning, and this has resulted in pressure to move from its traditional teaching model to more widespread electronic presentation of courses. At the same time a raft of new legislation and regulation now applies to electronic presentation. Thus the problem of electronic presentation of courses would seem to fit the characteristics of a type of problem to which the PDCA cycle could usefully be applied.

Back